IdPCertRenew

Regenerating Key/Certificate Pairs

IdP versions 2.3 and later

If you need to regenerate the key material that your IdP uses to communicate with other SPs (for instance because of key compromise or Federation Operator's restrictions), you can do so by using a variant of the installation script.

1. Change into the IdP distribution directory, shibboleth-identityprovider-VERSION. *This is the directory you created when you installed or last updated the IdP*.
2. Run either **`./install.sh renew-cert`** (on Unix systems) or **`install.bat renew-cert`** (on Windows systems).
3. Respond to the prompts appropriately.

The new private key, long lived certificate, and keystore files will be generated with the file name suffix '.new' in the directory you supplied to the script

To use this key/certificate pair, you must first update the IdP's metadata and publish the result. Then rename the files so they don't have the '.new' suffix, and configure them into your IdP. You will need to restart the Java servlet container for the IdP to pick up the new configuration.

The lifetime of the generated certificate can be changed from the default by setting the environment variable **`IdPCertLifetime`** to the number of years lifetime required before you run the script.